Introduction To

FAILURE MODES AND EFFECTS ANALYSIS

FMEA

IN AVIONICS

BY
THOMAS VEHUS 1999

Introduction to FMEA

Introduction and definition of terms

In order to get an airworthiness approval for an avionics system, a component manufacturer has to prove that their component meets the requirements set by the FAA/CAA. More specific they have to prove that the functions that their component performs, will not be lost or supply misleading information. To prove this, a mathematical tool exists. The FAA/CAA has set up and categorized failure-rates for these functions. These failure rates represent the probability for a system to fail. If the requirement for a system to fail is 10^{-7} per flighthour, then this system is "allowed" to fail once every 10 million flighthour. The probabilities are mathematical values that represent the category of criticality and the category of effect. The table below shows these failure-rate categories.

Failure rate per Flight hour	10^{-3}/H	10^{-5}/H	10^{-7}/H	10^{-9}/H
FAR probability	probable	improbable		extremely improbable
Cat. of Criticality	non essential	essential		critical
Cat. of Effect	Minor	Major	Hazardous	Catastrophic

Table 1 failure rate categories

As we can see from the table, a failure rate of 10^{-7} per flighthour is classified as an improbable event, this classification is used where the effect of the situation if the event should occur, would be hazardous. The criticality of the function that the system performs would in this case be essential. To determine the failure mode criticalities, the FAA/CAA has described the categories and published a list of functions and their respective categorizations. Below is a listing of some descriptions: Ref: AC 25-11

No effect: Failure conditions that do not affect the operational capability of the aircraft or increase pilot workload.

Minor: Failure conditions which would not significantly reduce aircraft safety, and which would involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload such as routine flight plan changes, or some inconvenience to occupants.

Major: Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.

Hazardous: Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be:

A large reduction in safety margins or functional capabilities

Physical distress or higher workloads such that the flight crew could not be relied on to perform their tasks accurately or completely.

Adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.

Catastrophic: Failure conditions which would prevent continued safe flight and landing.

The FAA/CAA has defined two terms of requirement:

Loss of Function(LF), which reflects the system's availability.

Misleading Information or Hazardously Misleading information(HMI), which reflects the system's integrity.

These two terms reflects the total system's safety properties. In some cases the failure rates or level of criticality are different for the two.

SAFETY ASSESSMENT

Let us pick a function for our analysis. Choose the display of attitude; let's consider the requirements of this function. The function is considered as a critical function. The requirements for the system are:

Loss of Function(LF) must be *extremely improbable*(10^{-9}), because the effect would be *catastrophic*.

Hazardously Misleading Information(HMI) on both pilot and copilot simultaneously must be *extremely improbable*, but HMI on any single primary display must be *improbable*.

As a result of these requirements we have to prove that our system meets the requirements. To do this we have to perform a safety assessment. What should this assessment contain? How will we prove that our attitude display will not fail more often than once every billion flight-hour? One of the tools often used in avionics is the **Failure Modes and Effect Analysis (FMEA)**.

FMEA

The theory behind this analysis includes among other things, the presumption that a system is vulnerable to certain failure modes. The effects of these failure modes will be manifested in different function failures. A sum of specific failure modes will result in a specific effect (function failure).

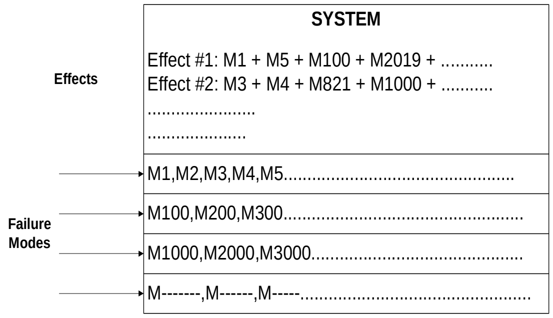
SYSTEM
Effects
Effect #1: M1 + M5 + M100 + M2019 + ...
Effect #2: M3 + M4 + M821 + M1000 + ...
....
....
Failure Modes
M1,M2,M3,M4,M5...
M100,M200,M300...
M1000,M2000,M3000..
M-------,M------,M-----..

Figure 1 Failure Modes and Effects.

For example, if failure mode M1 occurs, what will the effect of it be? Often will one failure mode cause a domino effect, and more failure modes will occur and make out a specific effect. In our example the effect is Loss of Function, which we decided to be display of attitude. We are looking for failure modes that causes loss of attitude display on both pilot and copilot side.

To proceed with our analysis we have to choose between two types of FMEA:

Top Down FMEA is used when it is desirable to evaluate one effect. The analysis starts with this effect and finds the failure modes.

Bottom Up FMEA is used when we want to find all the effects caused by all failure modes.

When it comes to certifying a system, it is often considered more desirable to use the Top Down approach. This is because we know which effect we have to meet the requirements for. It would be of great importance to find the failure modes, so that we can eliminate, or minimize them. It is also more time- and work- consuming to use the Bottom Up approach, and in aviation time **is** money.

TOP DOWN LOSS OF FUNCTION FMEA

Let us start the analysis by defining the system:

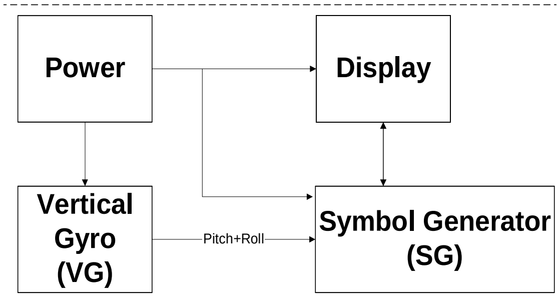

Figure 2 System description.

This is a **very** simple description of an attitude display system (attitude indicator). But basically such a system includes a power source, a sensor (vertical gyro), a symbol generator, and the display in the cockpit. Remember that this is only one side in the cockpit, the copilot will also have an identical independent system. This is required in passenger aircrafts by the FAA/CAA, to achieve a redundant system. This means that LF in our example is loss of **both** displays.

But we only have to calculate for one side and just include the other side in the final result, since they are identical. To start the analysis we choose one of the "black boxes" at a time and analyze the boxes successively to complete the analysis. In figure 3 I have chosen to start with the symbol generator.

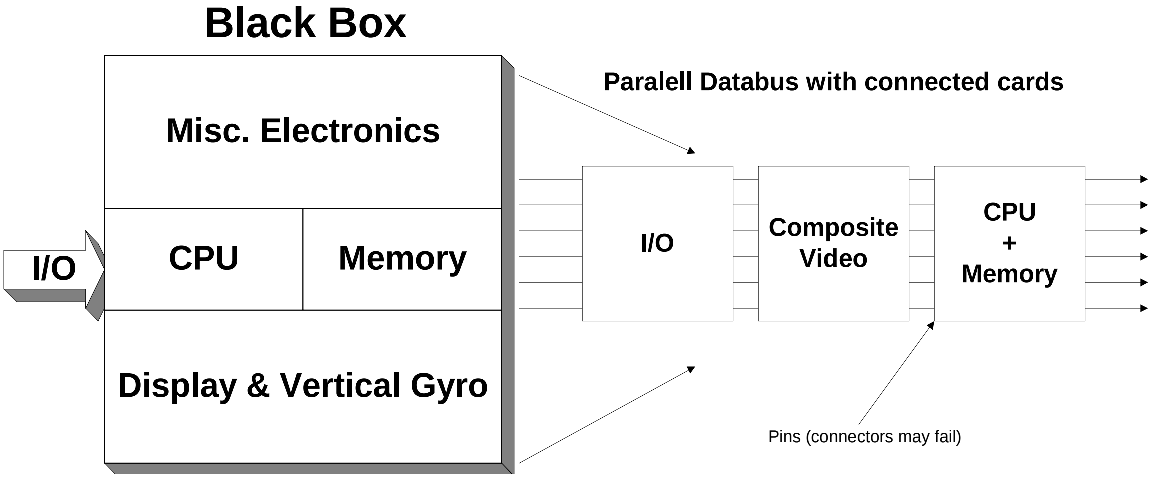

Figure 3 Component level analysis Symbol Generator

The next step is to choose one card at a time and analyze all of the cards successively. In my example I'll choose to start with the CPU + memory card. This is illustrated in figure 4.

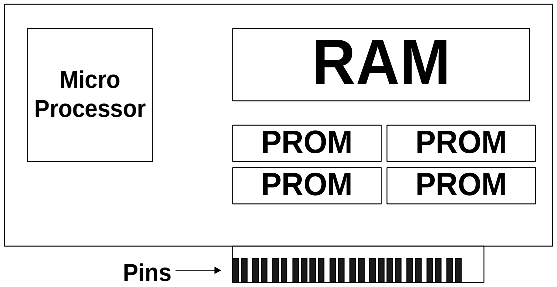

Figure 4 component level analysis, CPU + Memory Card

This card has pins, several PROMS, RAM and a CPU that all can fail. These are then failure modes of the card. As you might have understood by now: we take every potential failure mode and dissect it from top to bottom.

Assume that we have analyzed every possible failure mode, and that we have the failure rates for every component. The failure rates for specific components are available in:

MIL-HUBK-217E
Manufacturers own data
User data

We conclude that we have done a good job digging up all this information. But how shall we use it to find out if our system meets the requirements? The answer can be something called a **Fault-Tree analysis**.

FAULT-TREE ANALYSIS

A fault tree is used to visualize the data we found. The method makes extensive use of logical gates such as AND- and OR- gates. Figure 5 shows the complete, but very simplified fault tree of our problem. The fault tree method is a powerful but simple approach to a potentially hypercomplex analysis, and it is used extensively not only in aviation. The trick about setting up the fault tree, is to know whether several failure modes should be added or multiplied. The key is to think:

M1 **AND** M2 must simultaneously happen for the effect (LF) to occur. This means that we multiply the modes. If only one of the failure modes occurs, the resulting failure rate will be 0. For example both pilot **AND** copilot side must fail for LF to happen.

M1 **OR** M2 must happen for the effect(LF) to occur. This means that we add the modes. For example if either the CPU **OR** one of the memory modules on the card in figure 4 fail, it will make the card fail. It is sufficient that one of the failure modes of the card occurs to make the card fail.

As the figure shows: It is enough to calculate one of the sides in the cockpit. We just multiply them to find the LF probability. All values in figure 5 are **probabilities of failure per flight hour.**

PLEASE LOOK AT NEXT PAGE FOR THE FIGURE!

We stated earlier that the probability of LF attitude, loss of both attitude displays, had to be less than 10^{-9} per flighthour. Our analysis resulted in a probability per flighthour of $4.45*10^{-8}$; this is not good enough! We have not met the requirements. What can we do to improve our design, so that we can satisfy the FAA/CAA? Many answers can be found here, one way to do it is to add a third independent attitude indicator, as a backup, for example a mechanical indicator. If this indicator has a failure rate of say 10^{-3}, the resulting LF probability will be $2.11*10^{-4}$ **AND** $2.11*10^{-4}$ **AND** 10^{-3}, this gives a LF probability of $4.45*10^{-11}$. This satisfies the requirements. This method is often used in passenger aircrafts, merely to meet the certification requirements. A "good old" mechanical attitude indicator can in other words often be seen in new aircrafts with digital displays.

HMI analysis is similar to LF analysis. I will not explain that here. It is worth mentioning that HMI is performed on one side only.

That's it for now!

Thomas Vehus 1999
thomas_vehus@hotmail.com

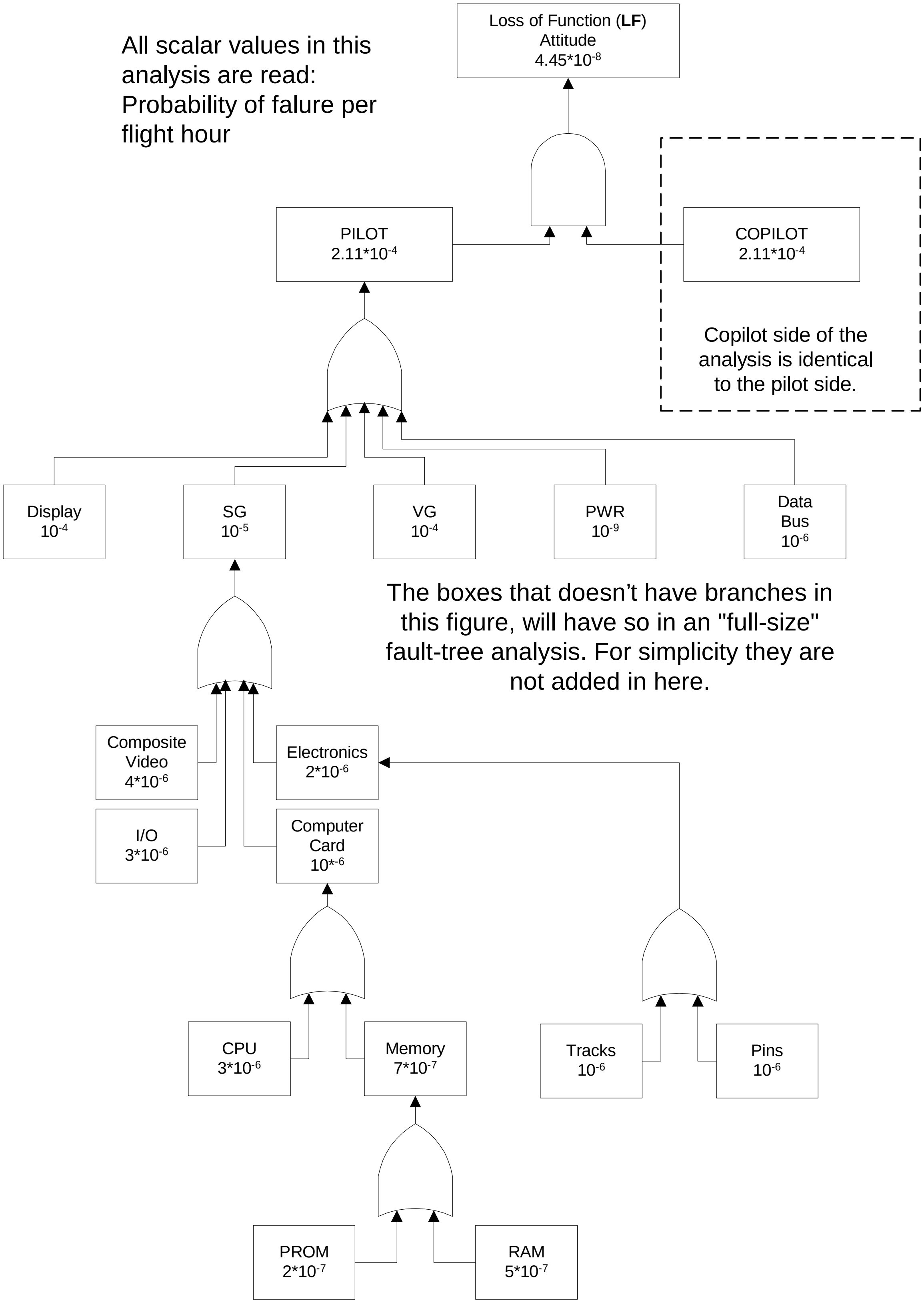
All scalar values in this analysis are read: Probability of falure per flight hour
Loss of Function (**LF**) Attitude 4.45*10-8
PILOT 2.11*10-4
COPILOT 2.11*10-4
Copilot side of the analysis is identical to the pilot side.
Display 10-4
SG 10-5
VG 10-4
PWR 10-9
Data Bus 10-6
The boxes that doesn't have branches in this figure, will have so in an "full-size" fault-tree analysis. For simplicity they are not added in here.
Composite Video 4*10-6
I/O 3*10-6
Electronics 2*10-6
Computer Card 10*-6
CPU 3*10-6
Memory 7*10-7
Tracks 10-6
Pins 10-6
PROM 2*10-7
RAM 5*10-7

Figure 5 Fault Tree Analysis